



# **ARIN Update**

**Summer 2011 JET Meeting**

**Mark Kusters  
Chief Technology Officer**

# Agenda

- DNSSEC
- RPKI
- In-addr.arpa transition
- Directory Service Stats (Whois-RWS)

# Changes Required to make DNSSEC work

- Transfer of in-addr.arpa to ICANN
- Signing in-addr.arpa, ip6.arpa and delegations that ARIN manages
- Provisioning of DS Records
  - ARIN Online
  - RESTful Interface (mid-september)
- All completed by 4/27/2011

# ARIN Online - Zone Management

ARIN  
American Registry for Internet Numbers

SEARCH WHOIS  [need help?](#)

NUMBER RESOURCES PARTICIPATE POLICIES FEES & INVOICES KNOWLEDGE ABOUT US

Welcome, dev

MESSAGE CENTER

WEB ACCOUNT

POC RECORDS

ORGANIZATION DATA

MANAGE RESOURCES

TRACK TICKETS

ASK ARIN

log out

IP6 ENABLED

MANAGE RESOURCES

Manage Reverse DNS

Using the text fields on the right, specify the hostnames (not the IP addresses) of the nameservers that should be authoritative for ALL the reverse DNS zones listed on the left. If you did not intend to specify a unified set of nameservers for all the reverse DNS zones listed on the left, then please press the CANCEL button to go back to the previous screen.

SELECTED ZONES IN - NET-64-112-0-0-1

0.112.64.in-addr.arpa.

1.112.64.in-addr.arpa.

2.112.64.in-addr.arpa.

3.112.64.in-addr.arpa.

4.112.64.in-addr.arpa.

5.112.64.in-addr.arpa.

6.112.64.in-addr.arpa.

7.112.64.in-addr.arpa.

8.112.64.in-addr.arpa.

9.112.64.in-addr.arpa.

10.112.64.in-addr.arpa.

11.112.64.in-addr.arpa.

12.112.64.in-addr.arpa.

13.112.64.in-addr.arpa.

14.112.64.in-addr.arpa.

HOSTNAMES OF NAMESERVERS

Nameserver 1: NS1.WEB-ZERO.NET

Nameserver 2: NS2.WEB-ZERO.NET

Nameserver 3: NS3.FOO.COM

Nameserver 4: NS4.BAR.COM

Nameserver 5: NS5.BLING.COM

Nameserver 6:

Nameserver 7:

Nameserver 8:

Nameserver 9:

Nameserver 10:

Nameserver 11:

Nameserver 12:

Nameserver 13:

CANCEL

SUBMIT

[Contact Us](#) [Terms of Service](#) [Media](#) [Site Map](#) [Search ARIN](#) [Privacy Statement](#) [Accessibility](#) [Network Abuse](#)  
© Copyright 1997 - 2010, American Registry for Internet Numbers

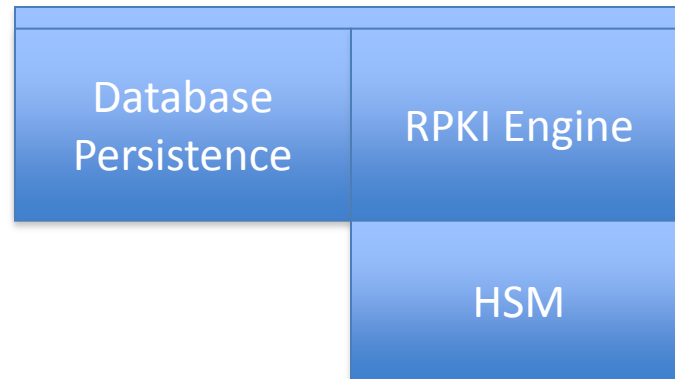
Version 2.6-SNAPSHOT build deployed 04-08-2010 14:27:33  
Conversation ID: 19 Long Running: true Pageflow: false

ARIN  
American Registry for Internet Numbers

# RPKI Pilot

- Available since June 2009
  - <http://rpki-pilot.arin.net>
  - ARIN-branded version of RIPE NCC software
- 45 organizations participating
- #2 (behind RIPE) on prefixes/roas

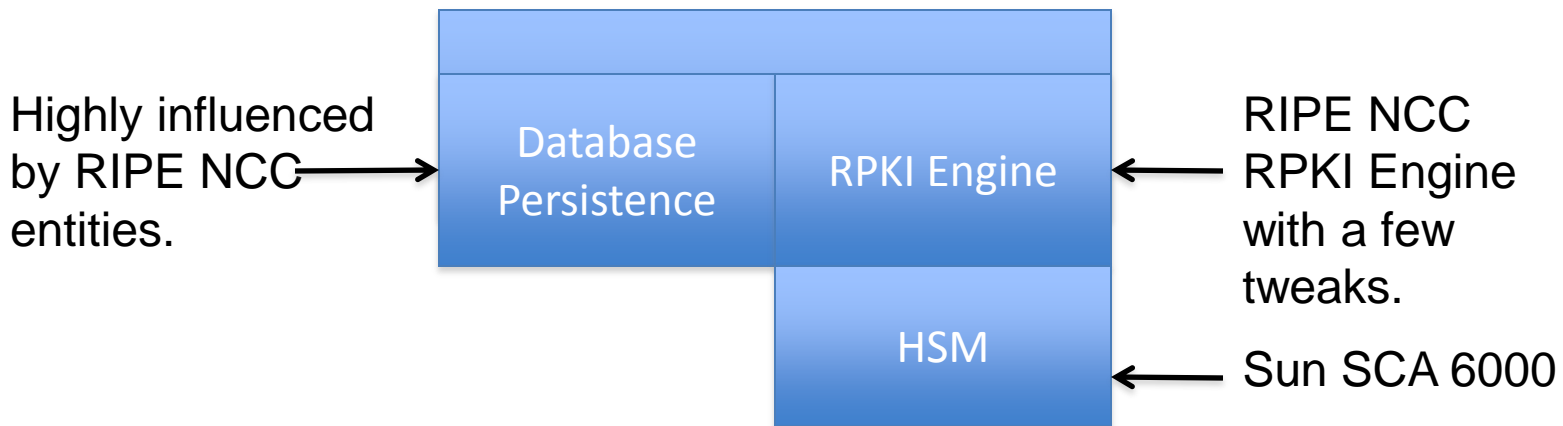
# General Architecture



Tight coupling between resource certificate / ROA entities and registration dataset at the database layer. Once certs/ROAs are created, they must be maintained if the registered dependents are changed.

# Development before ARIN XXVI

With a few finishing touches, ready to go Jan 1, 2011 with Hosted Model, Delegated Model to follow end of Q1.



Everything is Java, JBoss, Hibernate.

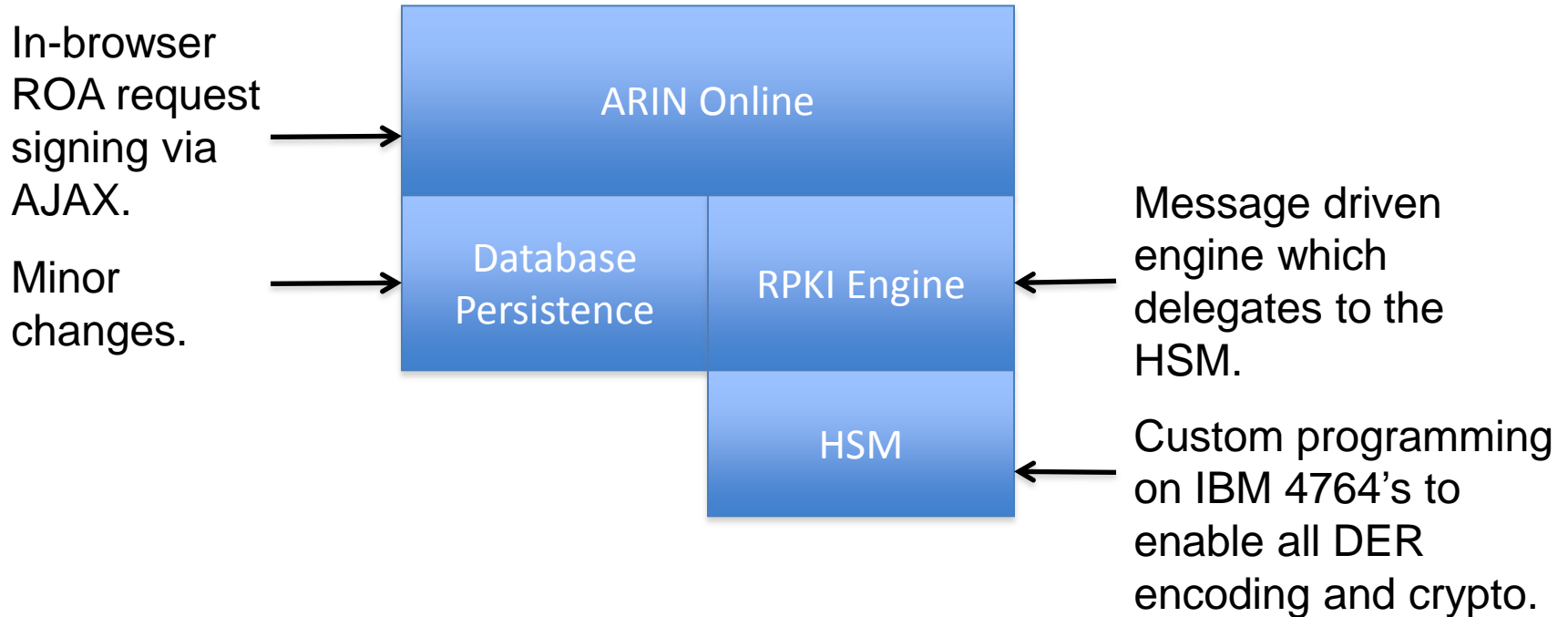
# From ARIN XXVI

- RPKI Services
  - ARIN to sign (assert) directly assigned/allocated resources
  - Other related services such as storing signatures/assertions for downstreams under review
  - Board of Trustees, along with ARIN General Counsel, are evaluating risks associated with these services
  - ARIN is seeking input from community regarding the these services

# As a Result...

- Completely new requirements for non-repudiation in ROA generation for hosted CAs
- Completely new requirements to thwart “Evil Mark” (rogue employee)
- Further intense review of liabilities by legal team and Board of Trustees

# Changes Underway



HSM coding is in C as extensions to IBM CCA. Libtasn1 used for DER coding.

# Example – Creating an ROA

ARIN  
American Registry for Internet Numbers

SEARCH Whois  
advanced search

NUMBER RESOURCESPARTICIPATEPOLICIESFEES & INVOICESKNOWLEDGEABOUT US

Welcome, Developer

MESSAGE CENTER (4)

WEB ACCOUNT

POC RECORDS

ORGANIZATION DATA

REQUEST RESOURCES

MANAGE RESOURCES

TRACK TICKETS

LISTING SERVICE

DOWNLOADS

ASK ARIN

log out

CREATE A ROUTE ORIENTATION AUTHORIZATION

There are two ways to submit a Route Origination Authorization (ROA) request.

**Browser Signed ROA Request:** Allows you enter in each required field separately and digitally sign the request with your RSA private key within the browser.

**Signed ROA Request:** Allows you to submit a digitally signed ROA request. This method requires you to construct a precisely formatted text block containing your ROArequest information, and then to sign it with and RSA private key which you create. More details on the formatting requirements are provided in a link in the signed ROA tab.

Submit Browser Signed ROA

Submit Signed ROA

\*Name:

\*Origin AS:

\*Validity Start Date:   
Enter the date in mm/dd/yyyy format.

\*Validity End Date:   
Enter the date in mm/dd/yyyy format.

Prefix:  /  Max Length  [Add](#)

Select Signing Private Key:  [Browse...](#) Key Not Loaded

This key will not be uploaded to ARIN.

\* denotes required field

SIGN AND CONTINUE

ARIN  
American Registry for Internet Numbers

File Upload

Computer > Win7 (C:) > projects > arin > arin\_developer\_trunk > keys

Organize > New folder

PerfLogs  
Program Files  
Program Files (x86)  
ProgramData  
projects  
.Net  
Airbus  
Android  
arin  
arin\_developer\_trunk  
.idea  
.svn  
arin\_commons.trunk  
arincore.trunk  
backoffice.trunk  
cert\_commons.trunk  
corews.trunk  
jpn\_ddl.trunk  
keys  
mgmt.trunk

Name	Date modified	Type	Size
filein	1/21/2011 9:53 AM	File	1 KB
fileout	1/21/2011 10:20 AM	File	1 KB
fileoutb	1/21/2011 8:48 AM	File	1 KB
key.pem	1/27/2011 1:36 PM	PEM File	1 KB
pk2.pem	1/27/2011 1:56 PM	PEM File	1 KB
pk3.pem	1/27/2011 1:29 PM	PEM File	1 KB
pk4.pem	1/27/2011 2:46 PM	PEM File	1 KB
pk5.pem	2/16/2011 11:45 AM	PEM File	1 KB
pk10.pem	2/15/2011 11:37 AM	PEM File	2 KB
pk11.pem	2/15/2011 11:42 AM	PEM File	1 KB
pub.key	1/24/2011 10:17 AM	KEY File	1 KB
pub10.pem	2/15/2011 11:38 AM	PEM File	1 KB
sign.bat	1/21/2011 10:21 AM	Windows Batch File	1 KB

File name: key.pem

All Files

OpenCancel

SEARCH Whois

advanced search

test with your RSA private

struct a precisely formatted  
ate. More details on the

\* denotes required field

SIGN AND CONTINUE

[Contact Us](#) [Terms of Service](#) [Media](#) [Site Map](#) [Search ARIN](#) [Privacy Statement](#) [Accessibility](#) [Network Abuse](#)

By using the ARIN Whois service, you are agreeing to the [Whois Terms of Use](#)

© Copyright 1997 - 2011, American Registry for Internet Numbers

Version 21.0-SNAPSHOT build deployed 04-07-2011 11:59:38

ARIN

American Registry for Internet Numbers

Welcome, Developer

MESSAGE CENTER (4)

WEB ACCOUNT

POC RECORDS

ORGANIZATION DATA

REQUEST RESOURCES

MANAGE RESOURCES

TRACK TICKETS

LISTING SERVICE

DOWNLOADS

ASK ARIN

[log out](#)

## CREATE A ROUTE ORIENTATION AUTHORIZATION

There are two ways to submit a Route Origination Authorization (ROA) request.

**Browser Signed ROA Request:** Allows you enter in each required field separately and digitally sign the request with your RSA private key within the browser.

**Signed ROA Request:** Allows you to submit a digitally signed ROA request. This method requires you to construct a precisely formatted text block containing your ROA request information, and then to sign it with and RSA private key which you create. More details on the formatting requirements are provided in a link in the signed ROA tab.

**Submit Browser Signed ROA**

**Submit Signed ROA**

\*Name:

\*Origin AS:

\* denotes required field

\*Validity Start Date:

Enter the date in mm/dd/yyyy format.

\*Validity End Date:

Enter the date in mm/dd/yyyy format.

Prefix:  /  Max Length  [Add](#)

Select Signing Private Key:

**Key Loaded**

[Click to Remove](#)

This key will not be uploaded to ARIN.

**SIGN AND CONTINUE**

Welcome, Developer

[MESSAGE CENTER \(4\)](#)

[WEB ACCOUNT](#)

[POC RECORDS](#)

[ORGANIZATION DATA](#)

[REQUEST RESOURCES](#)

[MANAGE RESOURCES](#)

[TRACK TICKETS](#)

[LISTING SERVICE](#)

[DOWNLOADS](#)

[ASK ARIN](#)

[log out](#)

## CREATE A ROUTE ORIENTATION AUTHORIZATION

There are two ways to submit a Route Origination Authorization (ROA) request.

**Browser Signed ROA Request:** Allows you enter in each required field separately and digitally sign the request with your RSA private key within the browser.

**Signed ROA Request:** Allows you to submit a digitally signed ROA request. This method requires you to construct a precisely formatted text block containing your ROArequest information, and then to sign it with and RSA private key which you create. More details on the formatting requirements are provided in a link in the signed ROA tab.

**Submit Browser Signed ROA**

**Submit Signed ROA**

\*Name:

\*Origin AS:

\* denotes required field

\*Validity Start Date:

Enter the date in mm/dd/yyyy format.

\*Validity End Date:

Enter the date in mm/dd/yyyy format.

Prefix:  / Max Length  [Add](#)

Select Signing Private Key:

**Key Loaded**

This key will not be uploaded to ARIN.

**SIGN AND CONTINUE**

Welcome, Developer

MESSAGE CENTER (4)

WEB ACCOUNT

POC RECORDS

ORGANIZATION DATA

REQUEST RESOURCES

MANAGE RESOURCES

TRACK TICKETS

LISTING SERVICE

DOWNLOADS

ASK ARIN

[log out](#)

## CREATE A ROUTE ORIGATION AUTHORIZATION

### SUBMIT SIGNED ROUTE ORIGATION AUTHORIZATION

Verify the information below matches the request you wish to submit, then click the button below. **Note: Your digital signature will not be validated until you click the button below.**

Name: **Test ROA**

Origin AS: **123**

Validity Period: **04-07-2011 - 04-07-2015**

Resources: **174.128.0.0/23**

Signature: **vGNHCrOlqDUGfcJzRWwhJVITPXeyxhWtt79pyqa3UJISuhFbuh  
ZVQdlhJ1uRZszmmCM33EvOI6QoO/HMUw+WPw==**

**SUBMIT SIGNED ROA REQUEST**

Welcome, Developer

MESSAGE CENTER (4)

WEB ACCOUNT

POC RECORDS

ORGANIZATION DATA

REQUEST RESOURCES

MANAGE RESOURCES

TRACK TICKETS

LISTING SERVICE

DOWNLOADS

ASK ARIN

[log out](#)

## ROUTE ORIGATION AUTHORIZATION

### ROUTE ORIGATION AUTHORIZATION REQUEST SUBMITTED

Thank you for submitting your route origination authorization request. Your request has been assigned ticket number:

**[ARIN-20110407-X3](#)**

You can also view the status of your request using [Track Tickets](#).

# Updates within RPKI outside of ARIN

- The four other RIRs are in production with Hosted CA services
- Major routing vendor support being tested
- Announcement of public domain routing code support

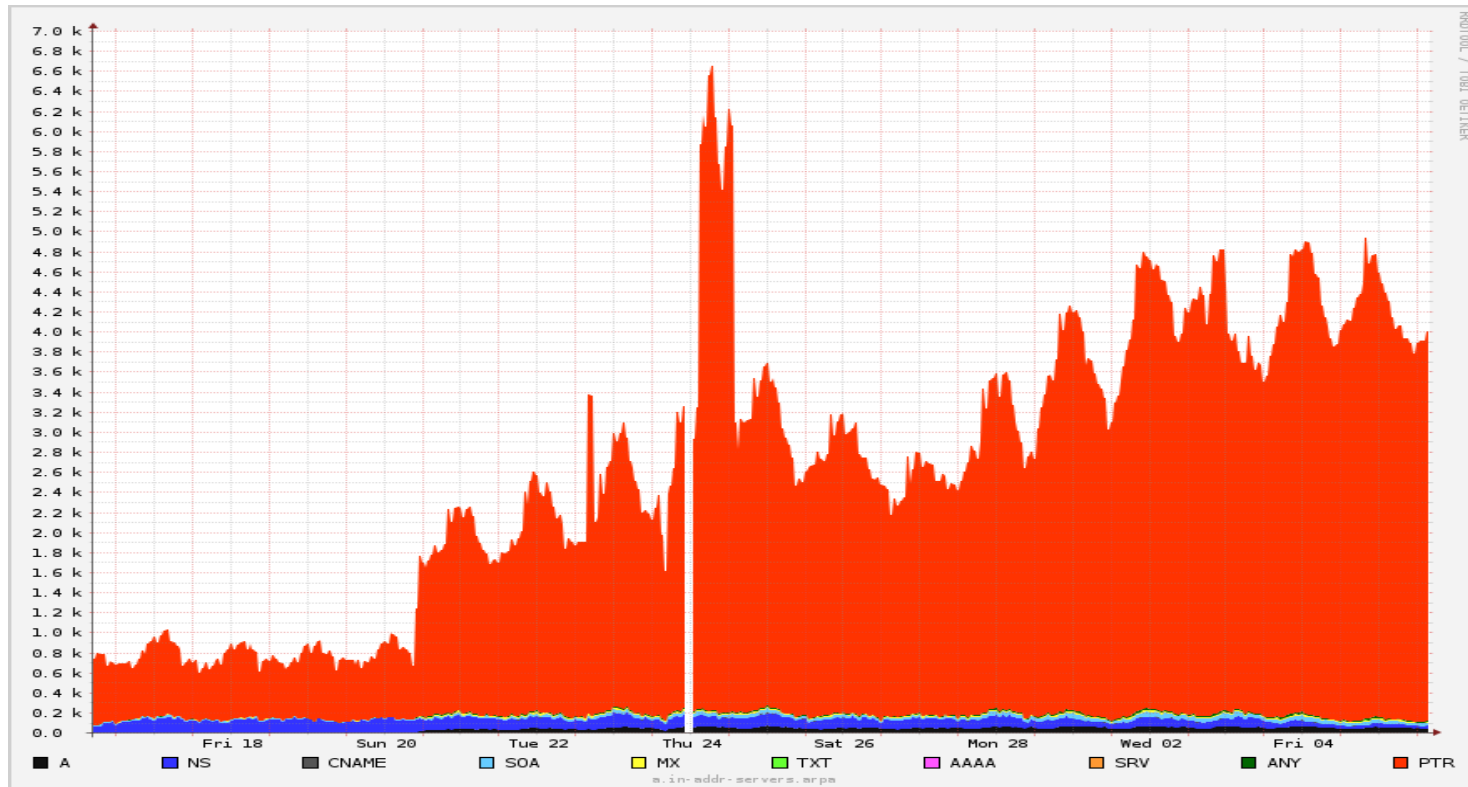
# ARIN Status

- Hosted CA anticipated by end of September at the earliest
- We intend to add up/down code for delegated model by the end of the year

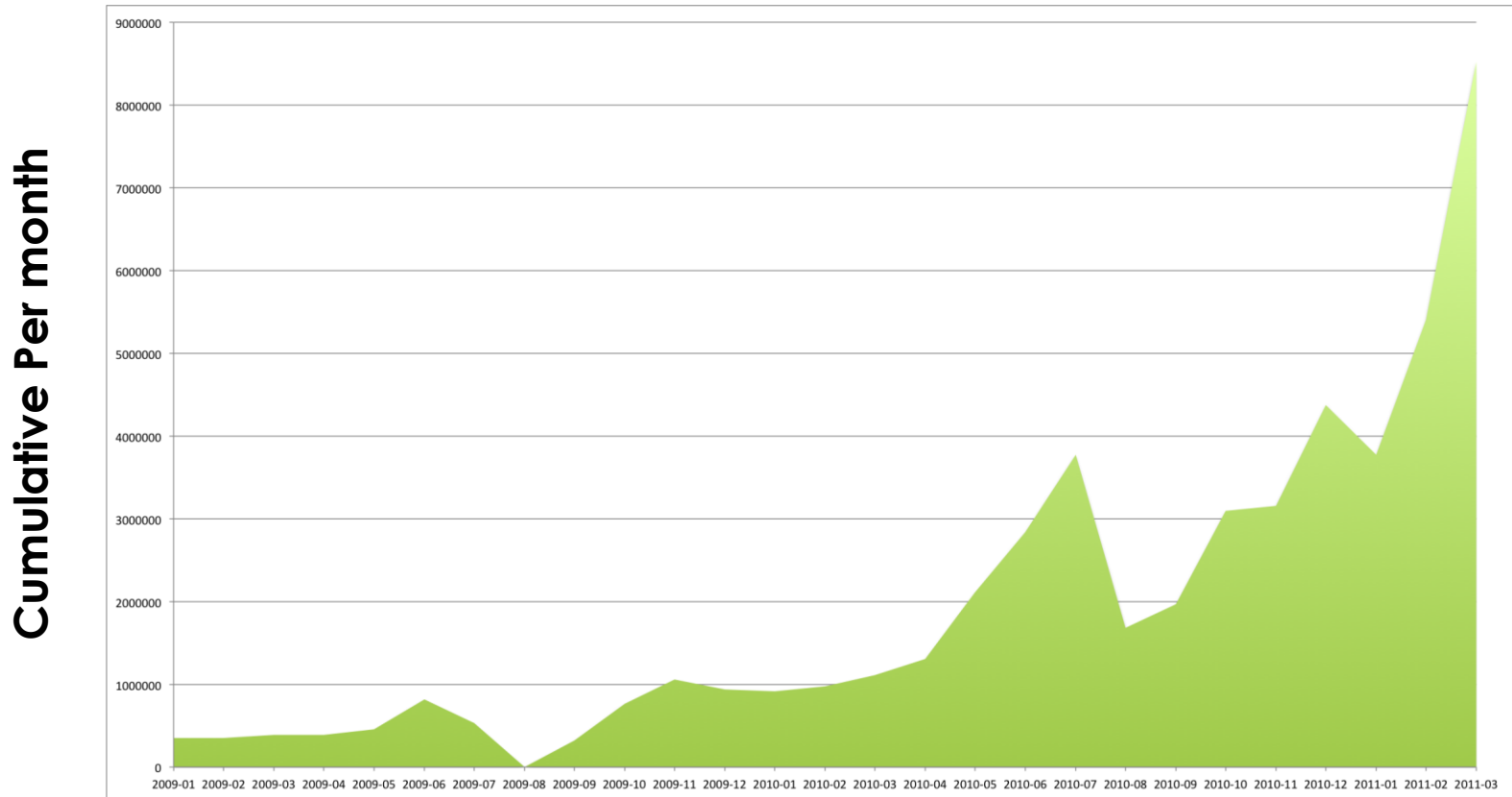
# in-addr.arpa Transition

- in-addr.arpa generation moved from ARIN to ICANN on 2/16/11
- in-addr.arpa moved from root servers to RIR/ICANN managed servers
- Servers moved off root in increments from 2/21/11 until 3/7/11
- in-addr.arpa is now signed
- Plan to provision DSs to ICANN for /8's under ARIN's control by 5/1/11
- No need for trust anchors by that point

# Traffic from a.in-addr-servers.arpa



# Whois-RWS Statistics – v6



# Whois/Whois-RWS Traffic Loads

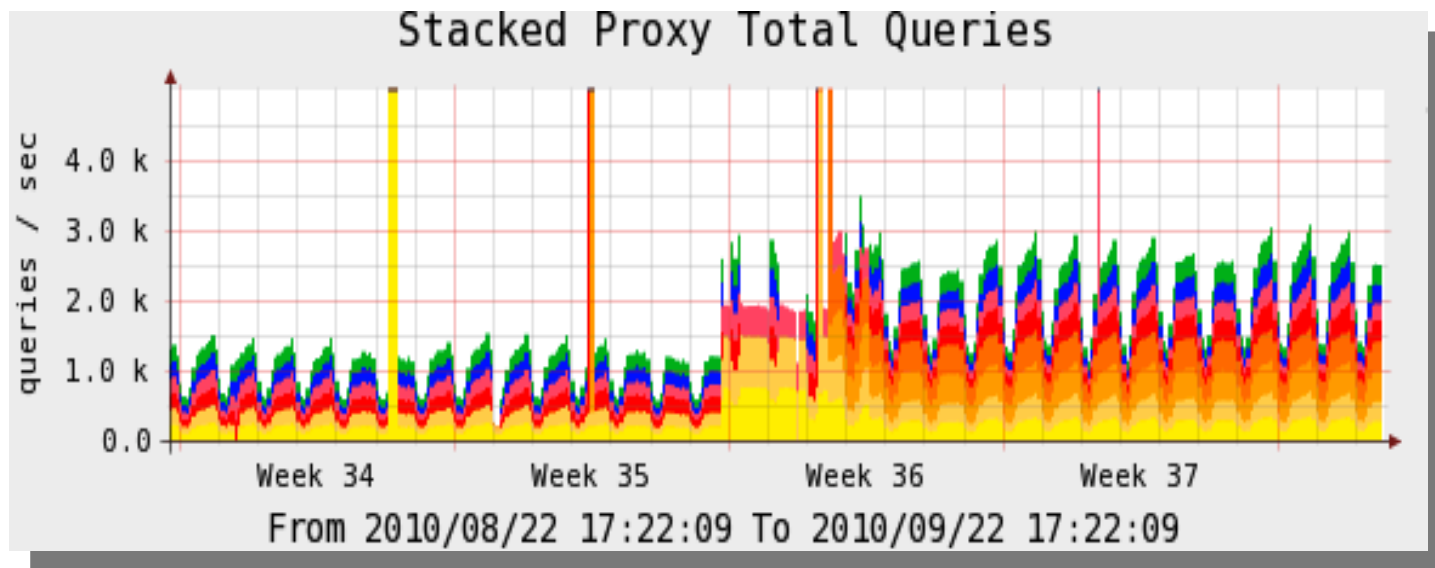
- Interesting traffic loads are dissipating
- Now versus 12 months ago
- At ARIN XXV
  - 50% of the queries are self-referential (i.e. source ip 192.168.2.5 asking for 192.168.2.5)
  - Most are singleton queries
  - Was increasing over the last year
  - Started noticing decrease after ARIN XXV

# Whois-RWS Traffic Loads

- **At ARIN XXVI**

- Saw a rise in traffic day after Google announced OpenID collaboration with Yahoo in September
- Traffic spiked 300%
- Top ten sites being login sites for various providers – Yahoo, AOL, and Facebook
- Approximately 5600 queries per second during the height of the day

# Whois-RWS Statistics- Uptick

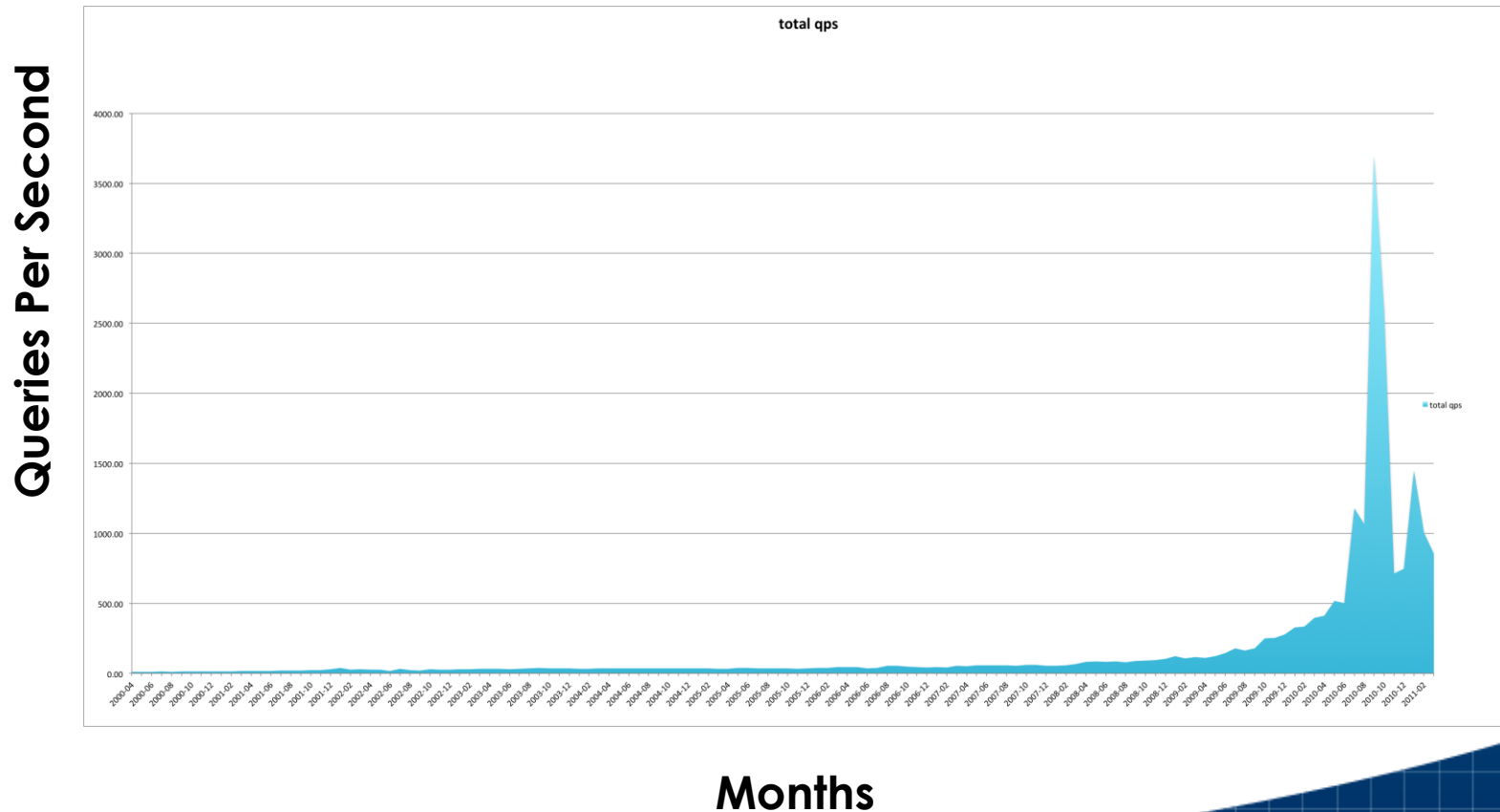


# Whois-RWS Loads

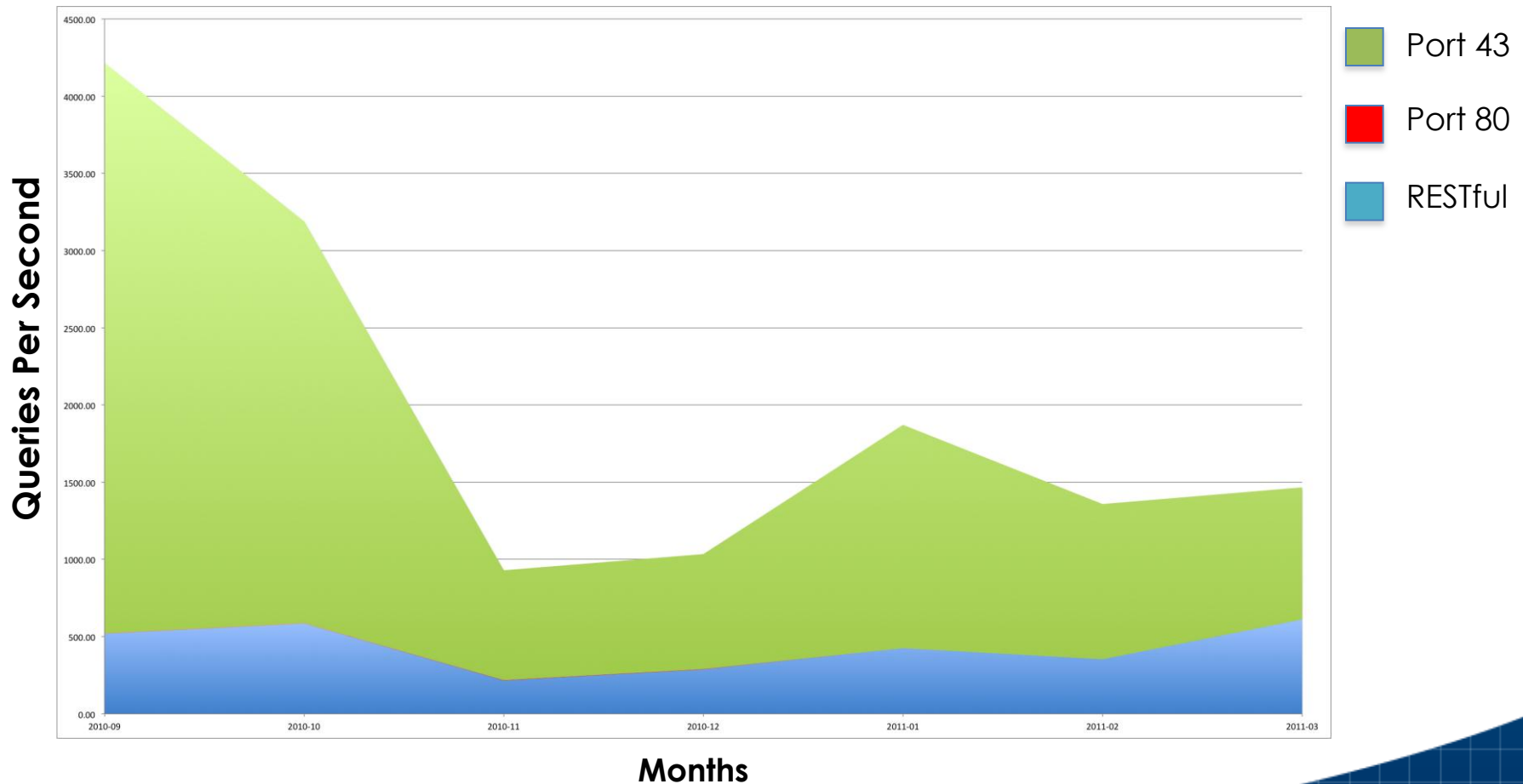
- Loads disappeared soon after ARIN XXVI
- Running “normally” now at 2000 queries per second

# Whois-RWS Statistics

## Whois Queries



# Cumulative Directory Service Traffic



# Thank You